# **گزارش آزمایش ششم**

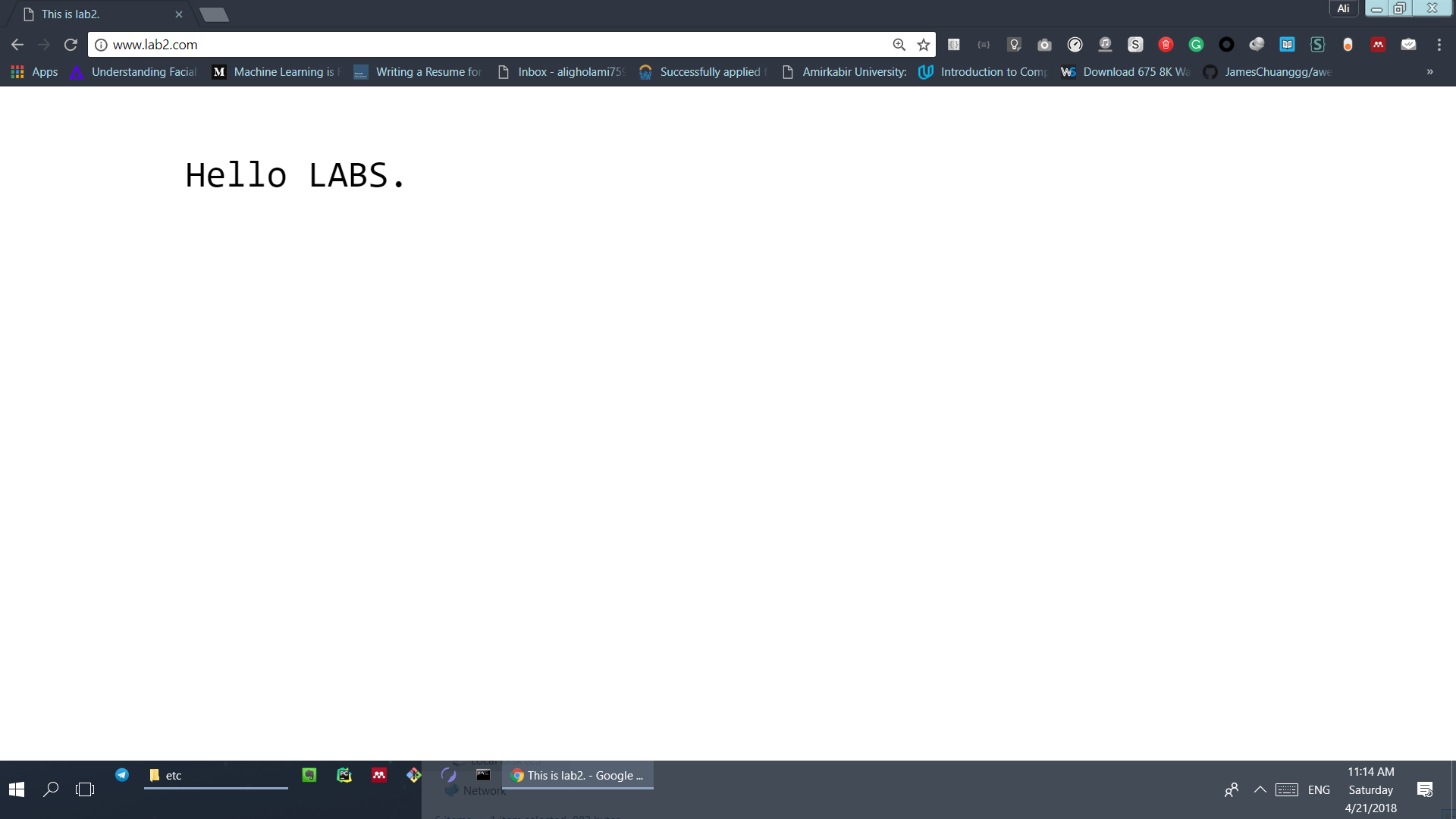
علیغلامی | شادی ابوالحسنی | احسان ولایی

# سوال اول: در مرورگر خود آدرس Host نوشته شده برای سایت را وارد کنید. سایتی که ایجاد کرده اید نمایش داده نمی شود. چرا؟

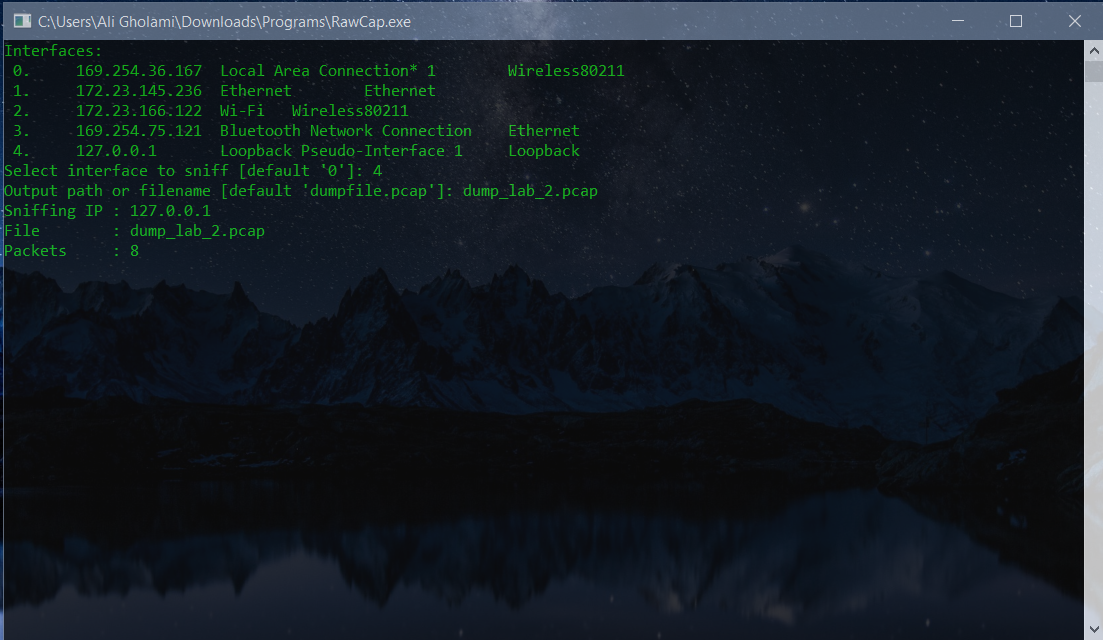
با توجه به اینکه هنوز آدرس IP سرور محلی ساخته شده با وجود نام دامنه ساخته شده برای سیستم نا شناس است. سیستم به فایل HOSTS رجوع می کند تا IP را از آنجا پیدا کند. فایل HOSTS نقش Local DNS Server را دارد.

# تصویر اول: سایت نمایش داده شده

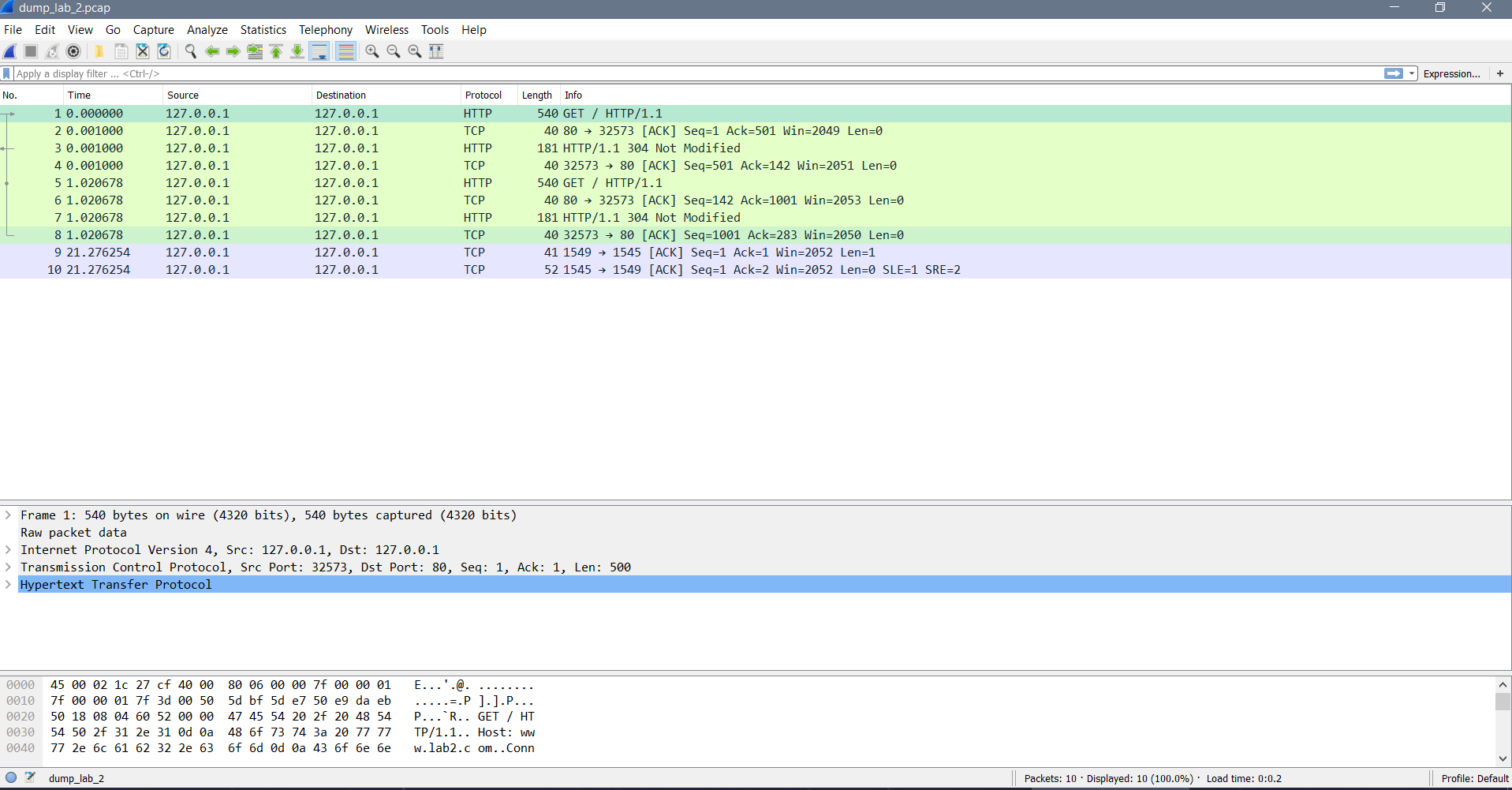
در تصویر زیر سایت را ملاحظه می فرمایید.



سوال دوم: ارتباط خود با سایت را با استفاده از Wireshark شنود کنید. آیا می توانید مشخص کنید کدام بسته مربوط به سایت شما است؟ چه اتفاقی افتاده است؟ با توجه به اینکه Loopback اتفاق افتاده است، Wireshark قادر به نمایش اطلاعات مربوط به بسته های Loopback نمی باشد. به بازگشت جریان داده ها یا سیگنال ها به مرجع خود Loopback اطلاق می شود.



سوال سوم: آدرس پورت های مبدا و مقصد چیست؟ روند برقراری ارتباط در پروتکل HTTP چگونه است؟ وب سرور چگونه آدرس سایت درخواستی شما را تشخیص می دهد؟ در تصویر زیر، اطلاعات مربوط به بسته های Loopback را که توسط Rawcap یافت شده است، ملاحظه می کنید.



آدرس پورت مبدا: 127.0.0.1:80

آدرس پورت مقصد: 127.0.0.1:80

ابتدا از طریق پورت 80 که مربوط به پروتکل HTTP می باشد، با وب سرور که روی پورت 32573 در حال شنود می باشد ارتباط TCP برقرار می شود. وب سرور نیز فایل index را برای درخواست خود ارسال می کند. آدرس سایت درخواستی همانطور که گفته شد از قبل در به عنوان یک DNS Domain Name در فایل HOSTS وارد شده است که وب سرور با آن متوجه می شود باید سایت [www.lab2.com](http://www.lab2.com) را لود کند.

سوال چهارم: یک سایت دیگر با نام دلخواه ایجاد کنید و بسته های مربوط به آن را شنود کنید. چه تفاوتی بین این دو سایت وجود دارد؟

تفاوت این دو سایت در HOST NAME آنها می باشد.

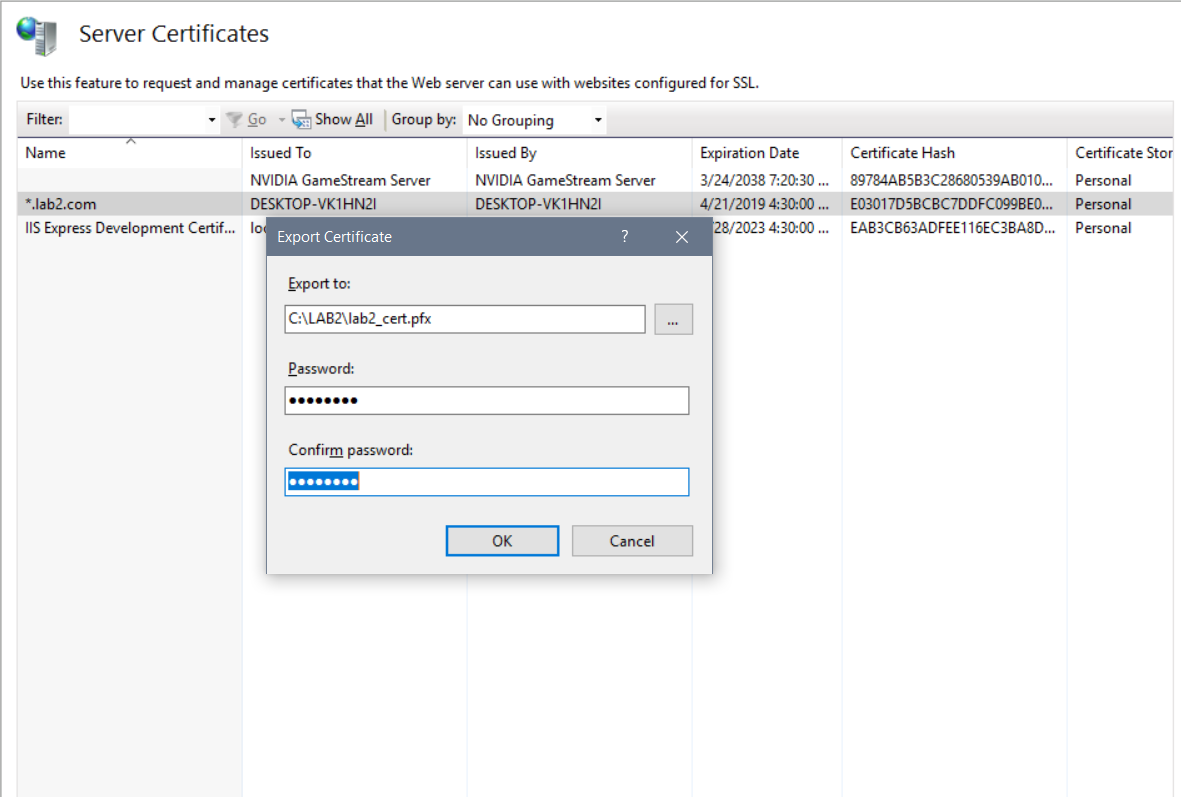
سوال پنجم: در مرورگر آدرس 127.0.0.1 را تایپ کنید. چرا هیچ کدام از سایت ها نمایش داده نمی شوند؟

با توجه به اینکه هر دوی آنها از پورت 80 استفاده می کنند، سایت نمایش داده نمی شود. به عبارتی، Address Conflict رخ می دهد.

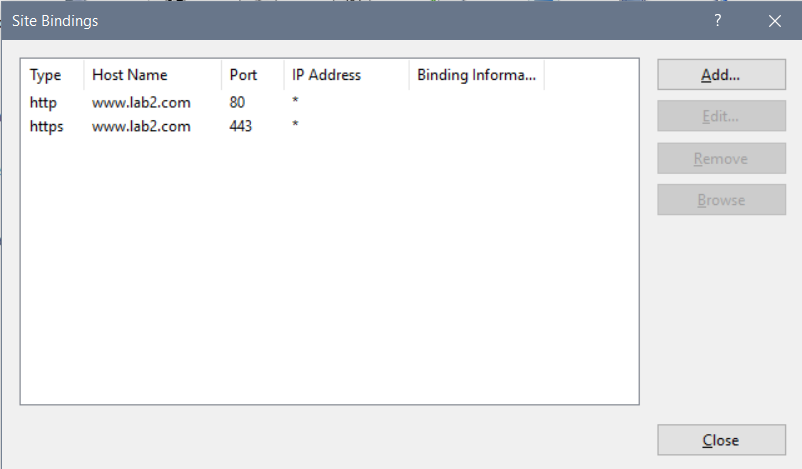
سوال ششم: در مرورگر آدرس 127.0.0.1 را تایپ کنید. چرا هیچ کدام از سایت ها نمایش داده نمی شوند؟

با توجه به اینکه هر دوی آنها از پورت 80 استفاده می کنند، سایت نمایش داده نمی شود. به عبارتی، Address Conflict رخ می دهد.

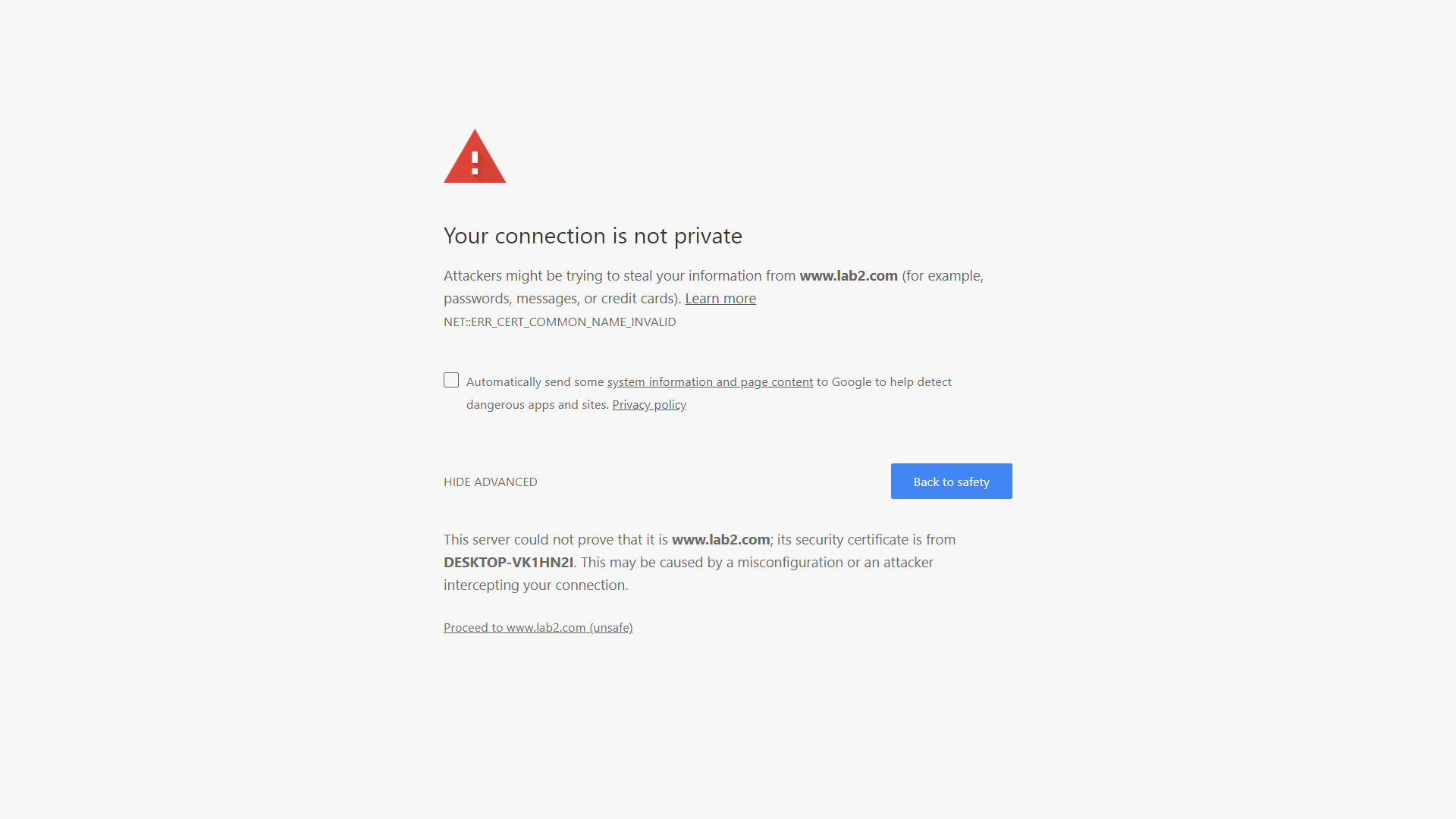
تصویر دوم: ایجاد یک گواهینامه



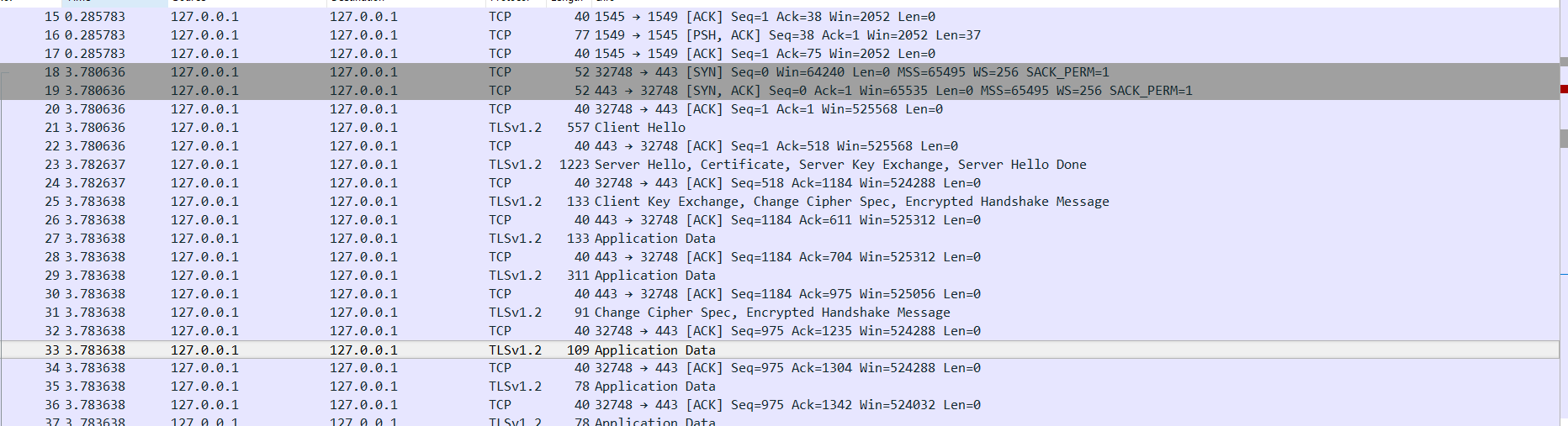
تصویر سوم: ایجاد یک بایندینگ Https برای وبسایت



تصویر چهارم: خطای Not Private Connection و اطلاعات گواهینامه



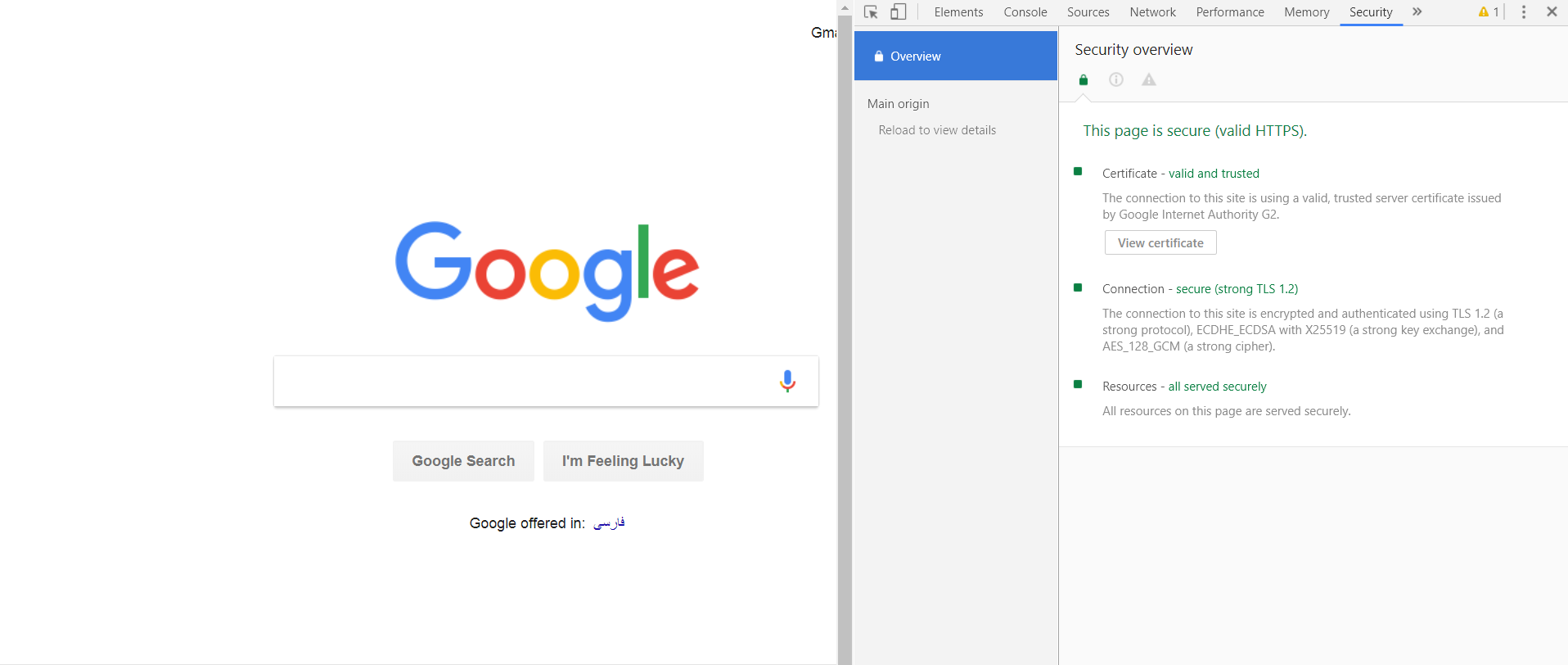
تصویر پنجم: اطلاعات بدست آمده از شنود پیغام ها بعد از ایجاد گواهینامه HTTPS



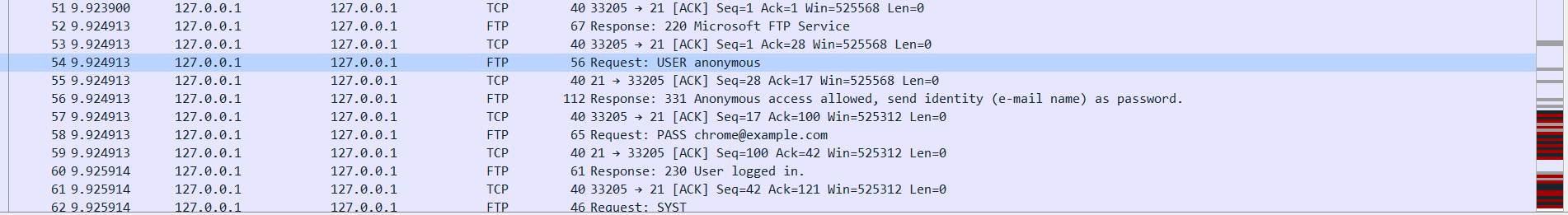
سوال هفتم: حال ارتباط را با Rawcap شنود کنید. بر روی بسته TLS مربوط به این ارتباط کلیک راست کرده و Follow SSL Stream را انتخاب کنید. آیا می توانید محتوی را ببینید؟

خیر، با توجه به اینکه محتوی Encrypt شده است، امکان دیده شدن آن وجود ندارد.

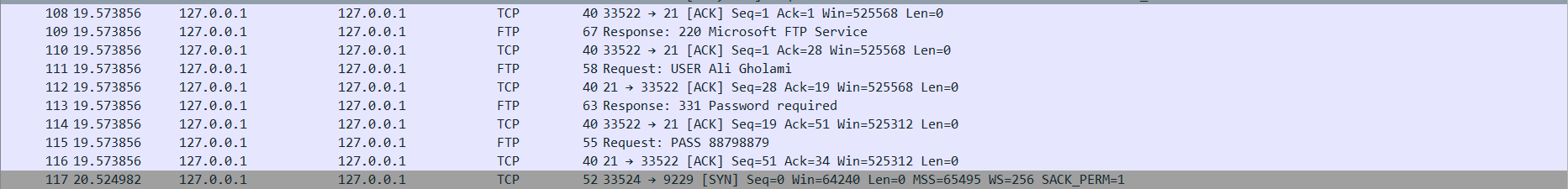
سوال هشتم: به سایت <https://google.com> متصل شده و گواهینامه آنرا بررسی نمایید.



سوال نهم: به آدرس ftp://www.lab2.com بروید. ارتباط را با Rawcap شنود کنید. مشخص کنید چه دستوری برای لیست کردن فایل های دایرکتوری استفاده شده است. مشخص کنید چه نام کاربری برای دسترسی به سایت استفاده شده است.

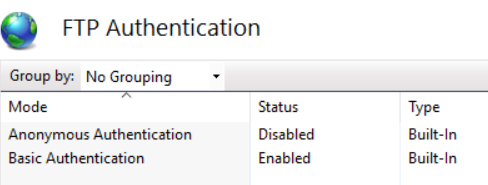


سوال دهم: دوباره به آدرس <ftp://www.test.com/> بروید. این بار باید نام کاربری و پسورد سیستم خود را وارد کنید تا اجازه دسترسی به شما داده شود. ارتباط را با Raw cap شنود کنید. آیا نام کاربری و پسورد قابل خواندن است؟



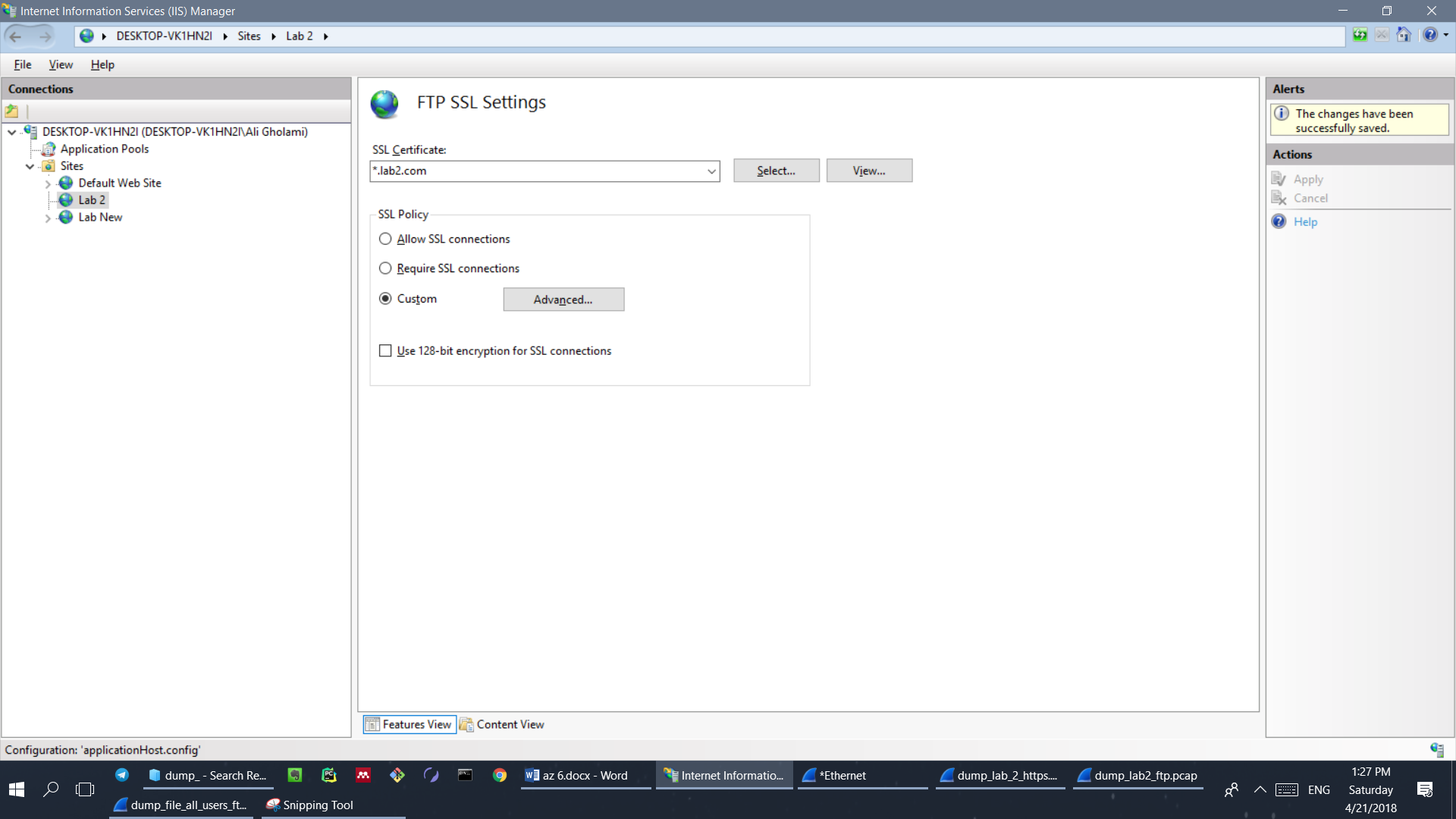
سوال یازدهم: به FTP Authentication و FTP Authorization وارد شوید و مشخص کنید چه سطح دسترسی برای چه کاربرانی تعریف شده است.

در اشکال زیر سطوح دسترسی را ملاحظه می کنید.





تصویر ششم: ایجاد یک SSL Certificate برای FTP



سوال دوازدهم: سعی کنید دوباره سایت را از مرورگر باز کنید. آیا می توانید به سایت وارد شوید؟ علت این خطا چیست؟

علت آن است که برای دسترسی به FTP در این حالت حتما باید گواهینامه معتبر SSL داشت.

سوال سیزدهم: برنامه FileZilla را از آدرس <https://filezilla-project.org/> دانلود کنید. پس از نصب، در قسمت Host، loopback را بنویسید. نام کاربری و پسورد ویندوز خود را وارد کنید و بر روی Quickconnect کلیک کنید. ارتباط را با Rawcap شنود کنید. آیا نام کاربری و پسورد قابل خواندن است؟

با توجه به اینکه از گواهینامه SSL استفاده می کنیم، اطلاعات قابل رویت نیستند.

